



[Desafío] CloudFormation



INTRODUCCIÓN

Este laboratorio es un entorno para crear una instancia de Amazon VPC y Amazon EC2 (y otros elementos de soporte) mediante una plantilla de AWS CloudFormation.

OBJETIVOS

- Crear y Una nube privada virtual de Amazon
- Una puerta de enlace de Internet conectada a la VPC
- Grupos de seguridad para acceder a la VPC configurados para permitir SSH desde cualquier lugar
- Una subred privada dentro de la VPC
- Una instancia de Amazon EC2 (una T3.micro) dentro de la subred privada (Nota: no es necesario acceder a EC2 a través de SSH o Escritorio remoto para una solución exitosa)



Desafío

En esta tarea, se ejecuta los comandos mediante AWS CLI para la creación de estos entornos.

- Después de iniciar el laboratorio, la terminal estará preconfigurada con las credenciales necesarias para usar la interfaz de línea de comandos de AWS (AWS CLI).
- La terminal también tiene instalado Python 3 con la biblioteca boto 3 disponible. Puede utilizarla para ejecutar el código del SDK de Python de AWS. Por ejemplo:

Descripción general del laboratorio

Este laboratorio es un entorno para crear una instancia de Amazon VPC y Amazon EC2 (y otros elementos de soporte) mediante una plantilla de AWS CloudFormation. El objetivo de este laboratorio es crear una plantilla de CloudFormation con los siguientes componentes:

- Una nube privada virtual de Amazon
- Una puerta de enlace de Internet conectada a la VPC



- Grupos de seguridad para acceder a la VPC configurados para permitir SSH desde cualquier lugar
- Una subred privada dentro de la VPC
- Una instancia de Amazon EC2 (una T3.micro) dentro de la subred privada (Nota: no es necesario acceder a EC2 a través de SSH o Escritorio remoto para una solución exitosa)

Cree y pruebe el laboratorio iterando la solución hasta que se creen todos los componentes. Informe al instructor cuando la plantilla se cree sin errores para que pueda revisar la solución completa.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Lab template

# Lab VPC with public subnet and Internet Gateway

Parameters:

  AmazonLinuxAMIID:
    Type: AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>
    Default: /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2

  LabVpcCidr:
    Type: String
    Default: 10.0.0.0/20

  PublicSubnetCidr:
    Type: String
    Default: 10.0.0.0/24

Resources:

#####
# VPC with Internet Gateway
#####
  MyS3Bucket:
    Type: AWS::S3::Bucket

  LabVPC:
    Type: AWS::EC2::VPC
```



```
Properties:
  CidrBlock: !Ref LabVpcCidr
  EnableDnsSupport: true
  EnableDnsHostnames: true
  Tags:
    - Key: Name
      Value: Lab VPC
```

```
IGW:
  Type: AWS::EC2::InternetGateway
  Properties:
    Tags:
      - Key: Name
        Value: Lab IGW
```

```
VPCtoIGWConnection:
  Type: AWS::EC2::VPCGatewayAttachment
  DependsOn:
    - IGW
    - LabVPC
  Properties:
    InternetGatewayId: !Ref IGW
    VpcId: !Ref LabVPC
```

```
#####
```

```
# Public Route Table
```

```
#####
```

```
PublicRouteTable:
  Type: AWS::EC2::RouteTable
  DependsOn: LabVPC
  Properties:
    VpcId: !Ref LabVPC
    Tags:
      - Key: Name
        Value: Public Route Table
```

```
PublicRoute:
  Type: AWS::EC2::Route
  DependsOn:
    - PublicRouteTable
    - IGW
  Properties:
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref IGW
    RouteTableId: !Ref PublicRouteTable
```



```
#####
# Public Subnet
#####

PublicSubnet:
  Type: AWS::EC2::Subnet
  DependsOn: LabVPC
  Properties:
    VpcId: !Ref LabVPC
    MapPublicIpOnLaunch: true
    CidrBlock: !Ref PublicSubnetCidr
    AvailabilityZone: !Select
      - 0
      - !GetAZs
        Ref: AWS::Region
  Tags:
    - Key: Name
      Value: Public Subnet

PublicRouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  DependsOn:
    - PublicRouteTable
    - PublicSubnet
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnet

#####
# App Security Group
#####

AppSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  DependsOn: LabVPC
  Properties:
    GroupName: App
    GroupDescription: Enable access to App
    VpcId: !Ref LabVPC
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 80
        ToPort: 80
        CidrIp: 0.0.0.0/0
  Tags:
```



```
- Key: Name
  Value: App
```

```
#####
```

```
# EC2 Instance in Public Subnet
```

```
#####
```

```
EC2Instance:
```

```
  Type: AWS::EC2::Instance
```

```
  Properties:
```

```
    InstanceType: t3.micro
```

```
    SubnetId: !Ref PublicSubnet
```

```
    ImageId: !Ref AmazonLinuxAMIID
```

```
    SecurityGroupIds:
```

```
      - !Ref AppSecurityGroup
```

```
    Tags:
```

```
      - Key: Name
```

```
        Value: Lab-EC2-Instance
```

```
#####
```

```
# Outputs
```

```
#####
```

```
Outputs:
```

```
  LabVPCDefaultSecurityGroup:
```

```
    Value: !Sub ${LabVPC.DefaultSecurityGroup}
```



Especificar plantilla [Información](#)

Una plantilla es un archivo JSON o YAML que describe los recursos y las propiedades de la pila.

Origen de la plantilla

Al seleccionar una plantilla se genera una URL de Amazon S3 donde esta se almacenará.

☐ URL de Amazon S3

Proporcione una URL de Amazon S3 a su plantilla.


☒ Cargar un archivo de plantilla

Suba la plantilla directamente a la consola.

☐ Sincronizar desde Git

Sincronice una plantilla de su repositorio de Git.

Cargar un archivo de plantilla

 Elegir archivo

lab-cloudformation-template.yaml



Archivo con formato JSON o YAML

URL de S3: Se generará cuando se cargue el archivo de plantilla

[Ver en Infrastructure Composer](#)

Especificar los detalles de la pila

Proporcionar un nombre de pila

Nombre de la pila

DesafioStack

El nombre de la pila debe tener entre 1 y 128 caracteres, comenzar con una letra y contener solo caracteres alfanuméricos. Recuento de caracteres: 12/128.



```
eee_W_3392514@runweb139567:~$ aws cloudformation describe-stacks --stack-name DesafioStack
{
  "Stacks": [
    {
      "StackId": "arn:aws:cloudformation:us-west-2:929401040301:stack/DesafioStack/91b
      fbb70-87a5-11ef-acbb-0ad25d875d35",
      "StackName": "DesafioStack",
      "Description": "Lab template",
      "Parameters": [
        {
          "ParameterKey": "LabVpcCidr",
          "ParameterValue": "10.0.0.0/20"
        },
        {
          "ParameterKey": "PublicSubnetCidr",
          "ParameterValue": "10.0.0.0/24"
        },
        {
          "ParameterKey": "AmazonLinuxAMIID",
          "ParameterValue": "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x8
6_64-gp2",
          "ResolvedValue": "ami-0992959aeea5762e8"
        }
      ],
      "CreationTime": "2024-10-11T07:51:05.778000+00:00",
      "RollbackConfiguration": {
        "RollbackTriggers": []
      },
      "StackStatus": "CREATE_COMPLETE",
      "DisableRollback": false,
      "NotificationARNs": [],
      "Outputs": [
        {
          "OutputKey": "LabVPCDefaultSecurityGroup",
          "OutputValue": "sg-0f537b68d2b8138a9"
        }
      ],
      "Tags": [],
      "EnableTerminationProtection": false,
      "DriftInformation": {
        "StackDriftStatus": "NOT_CHECKED"
      }
    }
  ]
}
eee_W_3392514@runweb139567:~$
```

DescribeStackResources	
AWS::EC2::SecurityGroup	CREATE_COMPLETE
AWS::EC2::Instance	CREATE_COMPLETE
AWS::EC2::InternetGateway	CREATE_COMPLETE
AWS::EC2::VPC	CREATE_COMPLETE
AWS::S3::Bucket	CREATE_COMPLETE
AWS::EC2::Route	CREATE_COMPLETE
AWS::EC2::RouteTable	CREATE_COMPLETE
AWS::EC2::SubnetRouteTableAssociation	CREATE_COMPLETE
AWS::EC2::Subnet	CREATE_COMPLETE
AWS::EC2::VPCGatewayAttachment	CREATE_COMPLETE